Southend-on-Sea Borough Council

Report of the Chief Executive

to

Cabinet

on
15 September 2020

Report prepared by:

John Williams, Executive Director (Legal and Democratic Services and Senior Information Risk Owner (SIRO)
Val Smith, Knowledge and Data Privacy Manager, Corporate Strategy Group

Cabinet Member – Cllr Gilbert

Information Governance Update and
Senior Information Risk Owner (SIRO) Annual Report 2019/20
Policy & Resources Scrutiny Committee

A Part 1 Public Agenda Item

1. Purpose of Report

1.1 To provide a summary of the Council's key actions in regard to information governance and management during 2019/20.
1.2 To report on opportunities and challenges in regard to information governance during 2020/21.
1.3 To comply with the requirement for the Senior Information Risk Owner (SIRO) to provide an annual report.

2. Recommendations

2.1 That the SIRO's report on Information Governance in Section 4 for 2019/20 be noted.

2.2 That the key actions taken during 2019/20, and the opportunities and challenges for 2020/21 be noted.

3. Background

3.1 The Council's Information Management Strategy was agreed by Cabinet in June 2016 and sets out the Council's vision for managing information, the principles supporting the vision and the context and challenges faced by the Council.

3.2 It also describes the related governance arrangements and action plan to progress the Council's approach and is complemented by a range of other strategies, policies and processes, notably Data Protection policies and procedures.

3.3 The Council's SIRO has overall responsibility for the Council's information management framework and acts as the champion for information risk within the Council. The SIRO for the Council is the Executive Director (Legal and Democratic Services).

3.4 The SIRO is responsible for producing an annual report on information governance. The report provides an overview of developments in relation to information governance, related work undertaken since April 2019 as well as outlining the strategic direction the Council has adopted. It should provide assurance that the Council's arrangements ensure personal data is held securely, information is disseminated effectively and that the Council is compliant with the legal framework - notably the General Data Protection Regulation (GDPR) and Data Protection Act 2018.

4.0 SIRO Annual Report – 2019-20

4.1 Leadership and Governance

4.1.1 The SIRO has to ensure that identified information threats and vulnerabilities are followed up for risk mitigation, and that perceived or actual information incidents are managed in accordance with Council's Risk Management Framework.

4.1.2 The SIRO's role is supported by:

- Two Privacy Officers (Data Controllers) - the Executive Director (Transformation), and the Director of ICT and Digital
- The Caldicott Guardian - the Director of Children's Services
- The Information Asset Owners (nominated officers)
- The Council's Data Protection Officer – Knowledge and Data Privacy Manager in the Corporate Strategy Group.

4.1.3 With regard to cyber security, the SIRO is supported by the Head of IT Security and Compliance. The ICT nominated cyber security specialists monitor developments; safeguard corporate systems and provide advice and training to the organisation concerning the responsibility of all staff to be aware of and to guard against cyber security threats. They also risk assess those aspects of Data Protection Impact Assessments which involve the use of such technology.

4.1.4 The Data Protection Officer (DPO) and their team assist the organisation in monitoring internal compliance, informing and advising on data protection obligations, providing advice, assistance and training on data protection matters and act as a contact point between the Information Commissioner and the Council. It is a statutory requirement that the DPO reports to the highest management level. Usually this is the Good Governance Group (GGG) but on occasions it will be the Corporate Management Team (of which the SIRO is also a part).

4.1.5 The DPO's team also manages Data Protection and Freedom of Information central records, monitors performance and compliance with legislation and leads on records management.

4.1.6 Leadership and governance of information management is provided by the Good Governance Group (GGG) whose remit includes information management along with the promotion of simple and effective governance.

4.1.7 The GGG is chaired by the SIRO, with membership including the SIRO, the Privacy Officers, the Caldicot Guardian and the DPO.

4.1.8 The Data Protection and Freedom of Information Community of Practice, led by the Knowledge and Data Privacy Manager, is a sub-group of the Good Governance Group. The COP monitors performance and has a focus on sharing good practice and its members provide expert knowledge to their colleagues. The SIRO is a member of the COP.

4.1.9 The Council is a signatory to the Whole Essex Information Sharing Framework (WEISF). The associated forum is known as the Wider Eastern Information Stakeholder Forum and is regularly attended by the Information Governance Advisor. Membership assists the Council in sharing best practice and in the appropriate sharing of personal data with public, third sector and contracted private organisations across Essex in a lawful, safe and informed way.

4.1.10 The Council is also a member of the Essex On-line Partnership which as part of its remit supports cyber security and the Information Governance Networking Group, a collection of data protection specialists who share practical advice and support in an informal environment.

4.2 Training and Awareness

4.2.1 Data Protection training continues to feature as a key part of ensuring staff are aware of their responsibilities.

4.2.2 During 2019/20 training through an e-learning platform was introduced. Modules covering data protection and cyber security are mandatory for all staff handling personal data. Staff who are less familiar with the use of computer-based learning are provided with supported training. For those with minimal personal data involved in their role, alternative provision is made to ensure that a level of understanding is reached appropriate to their responsibilities.

4.2.3 When examining data protection security incidents, the Data Protection Advisory Service routinely consider resultant training needs and bespoke training is provided as required.

4.2.4 Messages continue to be provided to staff alerting them to the need to protect personal data and use it appropriately. These have included a blog from the Data Protection Officer, posters emphasising the value of personal data, and all-staff messages.

4.2.5 In addition to the above, ICT have delivered training and awareness sessions specifically relating to cyber security and regular cyber security messages are issued by ICT to staff.

4.3 General Data Protection Regulation and Data Protection Act 2018

4.3.1 The European Union General Data Protection Regulation (GDPR) came into effect on 25 May 2018. The GDPR has direct effect across all member states and is the main point of reference for most data protection legal obligations.

4.3.2 The Data Protection Act 2018 (DPA 2018) also came into effect on that date. This details UK specific provisions allowed for by the GDPR and applies similar standards to GDPR to the handling of personal data which is not covered by EU law, for example to data relating to immigration.

4.3.3 The DPA 2018 also brought the EU Law Enforcement Directive into UK domestic law. This sets out the requirements for the processing of personal data for criminal law enforcement purposes and applies to the Council's regulatory activities which may result in criminal prosecution.

4.3.4 The DPA 2018 also covers the duties, functions and powers of the Information Commissioner (ICO) and the corresponding enforcement provisions.

4.3.5 The GDPR and DPA 2018 must be read side by side when considering the application of data protection legislation. Requirements concerning the proper use of personal data did not change upon the exit of the UK from the EU. This is because the UK government has committed to the adoption of the provisions of the GDPR into UK law and transitional arrangements have been agreed.

4.3.6 The position at the end of the transitional arrangements is currently unclear. It is probable that the UK will continue to use the standards of the GDPR and DPA 2018 to regulate activity within the UK and from the UK to the EU. It will depend upon the stance of the EU what the effect will be on data transfers from the EU to the UK.

4.3.7 An audit of the programme of work in preparation for GDPR was carried out in January 2019. It found that a comprehensive programme of work had been undertaken in advance of GDPR but there remained actions to embed GDPR as business as usual within the organisation. Progress against the audit has recently been reviewed and the remaining actions will be concluded in 2020/21. Progress against the associated action plan will be overseen by the Good Governance Group.

4.4 Data Security and Protection Toolkit

4.4.1 The Data Security and Protection Toolkit is an online tool that enables organisations to measure their performance against data security and information governance requirements which reflect legal rules and Department of Health policy. The Data Security and Protection Toolkit is the successor framework to the Information Governance Toolkit.

4.4.2 This independently audited self-assessment tool enables the Council to demonstrate that it can be trusted to maintain the confidentiality and security of personal information, in particular health and social care personal records.

4.4.3 The 2019/20 Toolkit was successfully completed. The Toolkit requires an independent audit of the Council's resulting self-assessment. This was conducted in February 2020 and it was confirmed with substantial assurance that the Council has appropriate evidence available for its assessment that the Toolkit standard was met.

4.5 Freedom of Information/Environmental Information

4.5.1 Under the Freedom of Information Act (FOIA) and Environmental Information Regulations (EIR), individuals are entitled to ask the Council for a copy of information it holds.

4.5.2 1227 requests were received in 2019/20, compared to 1480 in 2018/19. There has been a consistent reduction throughout the year in requests received. This may reflect greater transparency in the information provided by the Council through other means or it may be that levels have returned to a more normal level after a peak in the previous year.

4.5.3 To ensure consistency and compliance the FOI/EIR function is monitored within the Corporate Strategy Group (CSG). Requests are recorded centrally and then dispersed to departmental specialists for collation of data and for response. Where a response requires data from multiple departments, the response is collated by CSG. Advice on the use of any exemption from the requirement to provide information is also provided by CSG.

4.5.4 In 2019/20 the Council replied to 1245 requests, 67.07% within the required 20 working days. This compares to 1369 replied to in the previous year with 76.41% compliance. Consideration is being given to whether more data could be published to avoid the need for requests to be made.

4.5.5 While FOI/EIR requests do receive a response, too often it is outside the prescribed limit. This will require attention during 2020/21, see also Section 5 below.

4.6 Subject Access Requests

4.6.1 Under data protection legislation, individuals are entitled to ask the Council for a copy of the personal data it holds about them. This is known as a Subject Access Request (SAR).

4.6.2 There were 120 SARs received in 2019/20 an increase from 75 in the previous year. The increase may be because there is no longer a fee for making a request.

4.6.3 124 SARs were completed in 2019/20, an increase from 82 in the previous year. Some SARs are highly complex as they involve weighing the data protection rights of multiple data subjects within a record and may involve hundreds of documents. Responding within the required one month (or three months for complex cases) remains a challenge.

4.6.4 Additional resource has been continued to be allocated to increase the speed with which requests are processed however at the same time the volume of requests has increased considerably. See also Section 5 below.

4.7 Requests for Data Sharing

4.7.1 In 2019/20 a total of 313 individual requests for data sharing were received. Such requests are mostly received from the Police, for third party information. These requests are generally received through Legal and Democratic Services, Revenues and Benefits, Counter Fraud and Investigation and the Corporate Strategy Group.

4.7.2 Requests are centrally recorded to encourage consistency in decision making and to provide an audit trail in the event of a query regarding the appropriateness of data sharing.

4.7.3 Where information sharing is a regular occurrence, the Data Protection Advisory Service continues to work with service areas to introduce formal Information Sharing Agreements to promote clarity of responsibilities between all parties.

4.8 Data Security Incidents

4.8.1 In 2019/20 no data security incidents required notification to the Information Commissioner.

4.8.2 Increased data protection awareness within the organisation has resulted in an increase in investigations. Not all reported incidents will have resulted in a breach. Even where there is no breach, incidents can provide valuable insight into training requirements and processes and procedures which may need to be strengthened as a preventative measure.

4.9 Information Security (including Cyber Security)

4.9.1 The security function has been re-organised under the Head of IT Security and Compliance within the new ICT structure, with all existing resources aligned.

4.9.2 Development of a cyber security strategy is in progress, aligning the security program with the current threat landscape and risks to the organisation. This is assisting the prioritisation and planning of current delivery, as well as setting direction for the next 3-5 years.

4.9.3 Security processes and governance have been embedded across the key functional areas of ICT i.e. Business Partnering, Architecture, Delivery and Operations. Along with collaborative working with key stakeholders across the business e.g. Information Governance, Risk, Audit.

4.9.4 There has been significant support provided to delivery of business outcomes through tender and procurement processes, as well as the ongoing assurance and management of supplier security issues.

4.9.5 Cyber security operations and in particular incident response has been significantly stress tested during Covid-19 lockdown period, and through this we have refined our monitoring, handling and response playbooks to enhance our security posture.

4.9.6 A number of security improvements have been introduced in response to the changes in ways of working remotely and the technology provided, for example Multi-Factor Authentication has been implemented and adopted across our Office 365 users. An internal audit of the security of remote working is in progress and will report back through good governance group on assurance provided.

4.9.7 Awareness of cyber security matters has been enhanced through the introduction of mandatory e-learning and supplemented by regular communications on cyber related matters through the ICT weekly communications.

4.9.8 The cyber security threat landscape is actively monitored and emerging risk is identified and mitigated. To aid with this, intelligence is obtained from the National Cyber Security Centre (NCSC), Cyber Information Sharing Partnership (CISP) and Warning, Advice and Reporting Point (WARP) services.

4.9.9 Through the Local Government Association (LGA), Essex Online Partnership (EOLP) and NCSC networks we have had the opportunity to capitalise on grants, and funded initiatives as well as the full suite of NCSC services, for example:

- LGA grant for Cyber Security training and certification
- Metacompliance Phishing simulations and learning materials
- Network Early Warning System – vulnerability scans by NCSC

4.10 Records Management

4.10.1 With increasing public access to Council records, it is important that necessary documents are retained and that records are destroyed as part of a managed process that is adequately documented. Therefore, services must have in place clearly defined arrangements for the assessment and selection of records for disposal, and for documenting this work. All record keeping procedures must comply with the Council's Document Retention and Disposal Policy.

4.10.2 The Council has an Information Asset Register which acts as a mechanism for understanding and managing the Council's information assets and the risks to them.

5 Strategic Direction - Future Programme of Work

5.1.1 As 2020/21 began, the COVID-19 pandemic was developing. This has affected the priorities regarding information management and data security.

5.1.2 The majority of the Council's staff have suddenly become remote workers. This has provided challenges regarding the provision of remote access to Council systems. Access to hardcopy data is greatly reduced. Video conferencing has become common. Ways of carrying on business with customers while not being able to physically meet has had to be devised.

5.1.3 The Council has at short notice taken on new roles and responsibilities (for example the Coronavirus helpline including the provision of food deliveries and other support/new regulatory functions/local trace and track service) many of which have had to be newly devised, and has collaborated with both local and national bodies in order to respond quickly to circumstances as the pandemic has developed.

5.1.4 Despite the need for speed, it has been essential that each new addition has been properly assessed to ensure that the personal data of the people concerned is used correctly, is properly protected, is only used for the purpose for which it has been provided an only retained as long as is necessary. This has been a primary priority, as has the investigation and resolution of data and cyber security incidents.

5.1.5 Along with the rest of the nation, council staff have had their own challenges, becoming ill due to COVID-19, having to self-isolate, learning to work in a new environment, many having caring responsibilities as well. Some staff who usually have information management responsibilities have been redeployed to support high priority areas. Others who would normally provide content for information requests have had to prioritise front line services and support.

5.1.6 This has all taken its toll on the Council's ability to provide its service for FOI/EIR and Subject Access requests and other data subject rights. It has also impacted on the prioritisation of work from the GDPR Audit. While we have maintained all aspects of information governance, FOI/EIR and data protection work during the pandemic, usual timescales for compliance have unfortunately been a casualty on occasions.

5.1.7 The Information Commissioner has stated their intention to be a pragmatic regulator in these unprecedented times. It will be necessary however as the situation eases, to take stock of the situation and prepare a recovery plan to bring FOI/EIR, SAR and other data subject rights within their regulatory timeframes.

5.1.8 Through 2020/21 ICT will focus on delivery of technology within the existing data centres, cloud computing environments and ecosystems e.g. Office 365 to provide a greater level of currency, standardisation, and resilience. In doing so this will provide firm foundations for delivery of technology across the Council.

5.1.9 In step with the ICT technology delivery, the cyber security program will deliver a number of initiatives that further enhance our cyber resilience and response capabilities.

6 Other Options

6.1 It is a requirement of the Council’s Information Management Strategy that an annual report is made to councillors.

7 Reason for Recommendation

To ensure that the Council holds personal data securely; disseminates information effectively; is transparent and enabling in its handling of information and operates within the necessary legal framework.

8 Corporate Implications

8.1 Contribution to Southend 2050 Road Map

Many aspects of the Southend 2050 Road Map will be underpinned by technology and data. Sound information management and the proper protection of personal data therefore contributes to all aspects of the Southend 2050 work. Providing reliable information management which is trusted will contribute to the safety of residents and enabling technological advancements will contribute to making Southend a leading digital city.

8.2 Financial Implications

Any financial implications arising from this work will be considered through the normal financial management processes. Proactively managing information can result in reduced costs to the Council by reducing exposure to potential loss (such as fines from the Information Commissioner which could be up to £17million).

8.3 Legal Implications

Information management and data protection are subject to a range of legislation, including the General Data Protection Regulation and Data Protection Act 2018, as detailed in this report.

8.4 People Implications

Any people implications will be considered through the Council's normal business management processes.

8.5 Property Implications

None

8.6 Consultation

Internal

8.7 Equalities and Diversity Implications

Data Protection Policies and Procedures are available on the Council's website and transactional forms are included in MySouthend. Alternative channels remain available for those customers who may not be able to access or use digital services, and reasonable adjustments for disability are made where required.

8.8 Risk Assessment

Non-compliance with the law would adversely affect the Council's reputation in the community, reduce public trust and could lead to regulatory penalties and disruption to business continuity.

8.9 **Value for Money** – None identified

7.10 **Community Safety Implications** – None identified

7.11 **Environmental Implications** – None identified

8 Background Papers - None

9 Appendices - None